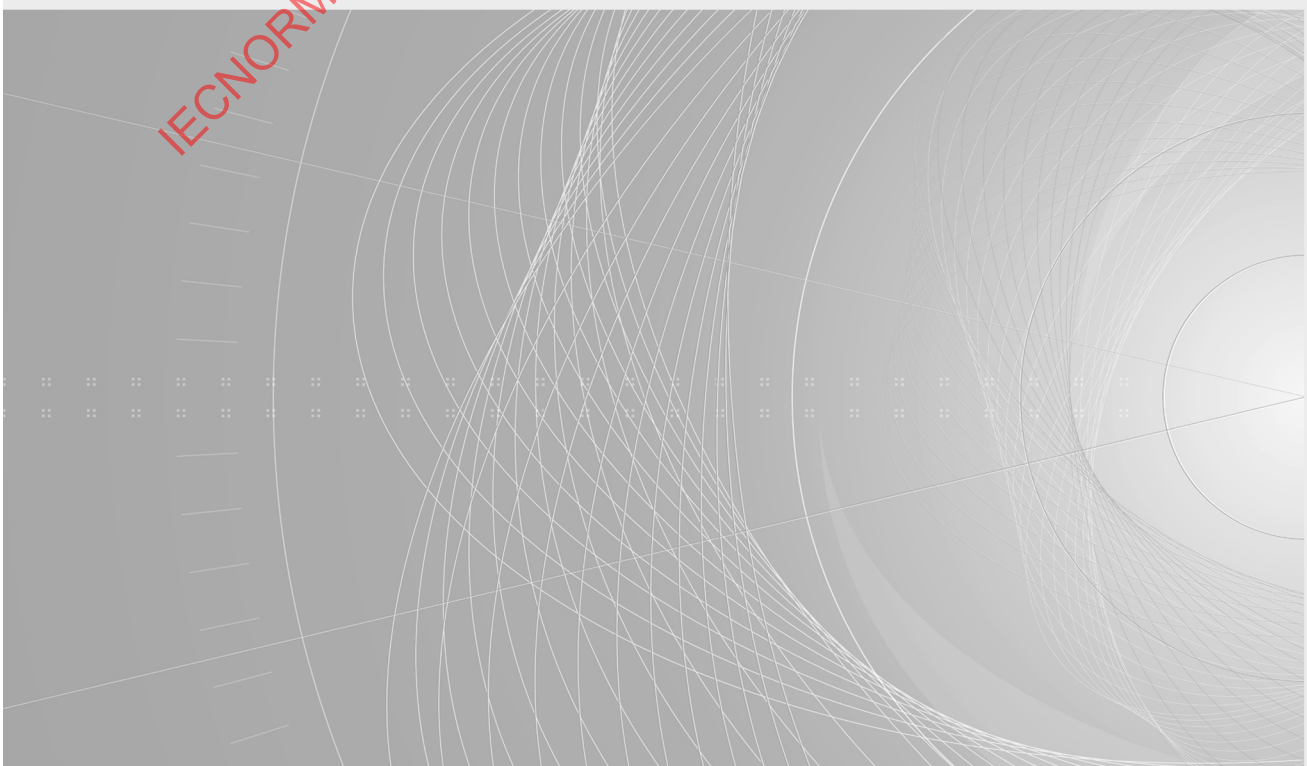
IEC TS 63208

Edition 1.0 2020-03

TECHNICAL SPECIFICATION

colour inside

Low-voltage switchgear and controlgear – Security aspects



IEC TS 63208:2020-03(en)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC TS 63208

Edition 1.0 2020-03

TECHNICAL SPECIFICATION

Low-voltage switchgear and controlgear – Security aspects

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 29.130.20

ISBN 978-2-8322-8021-8

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

LOW-VOLTAGE SWITCHGEAR AND CONTROLGEAR – SECURITY ASPECTS

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a Technical Specification when

– the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
– the subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical Specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC TS 63208, which is a Technical Specification, has been prepared by subcommittee 121A: Low-voltage switchgear and controlgear, of IEC technical committee 121: Switchgear and controlgear and their assemblies for low voltage.

The text of this Technical Specification is based on the following documents:

Draft TS	Report on voting
121A/321/DTS	121A/331A/RVDTS

Full information on the voting for the approval of this Technical Specification can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

The growing use of data communication capabilities by switchgear and controlgear (called “equipment” in this document) automatically increases cybersecurity risks. In addition, information technology is more often interconnected to and even integrated into industrial systems which therefore, increase this risk.

Very often, switchgear, such as circuit-breakers, or controlgear, such as overload relays or proximity switches, are equipped with data communication interface. They can be connected to a logic controller or remote display, with local and remote connectivity for giving access to data such as actual power supply values, monitoring data, data logging and remote upgrade.

For these typical applications for electrical distribution and machinery, minimum cybersecurity requirements are needed for maintaining an acceptable level of safety integrity of the protection functions for equipment, with or without data communication capability. These requirements are intended to limit the vulnerability of the data communication interfaces. To keep the largest freedom of innovation, the relevant requirements for a defined application are determined preferably by a systematic risk assessment approach.

The intention of this document is to:

1) develop an awareness of cybersecurity risks associated with unintended operation and loss of protective functions;
2) provide minimum cybersecurity requirements for equipment to mitigate the likelihood of unintended operation and loss of protective functions in the context of electrical distribution installations and control systems of machinery;
3) provide guidance to avoid impairing the functionality of equipment, in all operating modes, as a consequence of the implementation of security countermeasures.

This document gives guidance on countermeasures applicable to the design of the equipment (hardware, firmware, network interface, access control, system) and on additional countermeasures to be considered for the implementation and instruction for use. This document uses relevant references to ISO/IEC 27001, IEC 62443 (all parts) and IEC 62351 (all parts).

As a first stage, the content of this document is intended to be referenced by product standards. The common security requirement of IEC SC 121A product standards are expected to be moved to a future edition of IEC 60947-1.

LOW-VOLTAGE SWITCHGEAR AND CONTROLGEAR – SECURITY ASPECTS

1 Scope

This document applies to the security related main functions of switchgear and controlgear during the whole lifecycle of the equipment. It is applicable to wired and wireless data communication means and the physical accessibility to the equipment, within its limits of environmental conditions.

This document is intended to develop awareness about security aspects and provides recommendations and requirements on the appropriate countermeasures against vulnerability to threats.

In particular, it focuses on potential vulnerabilities to threats resulting in:

– unintended operation of the switching device or the control device or sensor, which can lead to hazardous situations;

– unavailability of the protective functions (overcurrent, earth leakage, etc.).

This document does not cover security requirement for information technology (IT) and for industrial automation and control systems (IACS), but it only implements in switchgear and controlgear appropriate security countermeasures derived from the base security publication ISO/IEC 27001 and the group security publications IEC 62443 (all parts).

This document, as a product security publication, follows IEC Guide 120 and includes typical use case studies as given in Annex B.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60364-7-729, *Low-voltage electrical installations – Part 7-729: Requirements for special installations or locations – Operating or maintenance gangways*

IEC 60947-1:2020, *Low-voltage switchgear and controlgear – General rules*

IEC 62443-4-1:2018, *Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements*

IEC 62443-4-2:2019, *Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components*

IEC TR 63201:2019, *Low-voltage switchgear and controlgear – Guidance for the development of embedded software*

ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*

FIPS 186-4, *Digital Signature Standard (DSS)*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1.1
audit log
logs collecting the evidence of selected user activities, exceptions, and information security events

Note 1 to entry: These logs are kept for an agreed period of time to assist in future investigations.

Note 2 to entry: Audit logs can be used to comply with legal requirements.

[SOURCE: ISO/IEC 24775-2:2014, 3.1.7]

3.1.2
attack
attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

[SOURCE: ISO/IEC 27000:2018, 3.2]

3.1.3
attack surface
set of attack points that an attacker can use in order to trigger an attack

[SOURCE: ISO/TS 12812-2:2017, 3.4, modified – "enter or capture data in an information system" replaced by "trigger an attack".]

3.1.4
attack vector
path or means by which an attacker can gain access to a device in order to generate an attack

[SOURCE: ISO/IEC 27032:2012, 4.10, modified – "computer or network server" replaced by "device" and "deliver a malicious outcome" by "generate an attack".]

3.1.5
authentication
security measure designed to establish the validity of a transmission, message, or originator

[SOURCE: IEC TS 62443-1-1:2009, 3.2.13, modified – Last part of the definition deleted.]

3.1.6
authenticity
property that an entity is what it claims to be

[SOURCE: ISO/IEC 27000:2018, 3.6]

3.1.7
authorization
right or permission that is granted to a system entity or an individual to access a system resource

[SOURCE: IEC TS 62443-1-1:2009, 3.2.14, modified – Addition of "or an individual".]

3.1.8
availability
property of being accessible and usable upon demand by an authorized entity

[SOURCE: ISO/IEC 27000:2018, 3.7]

3.1.9
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities or processes

[SOURCE: ISO/IEC 24767-1:2008, 2.1.2]

3.1.10
countermeasure
action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken

[SOURCE: IEC TS 62443-1-1:2009, 3.2.33, modified – Note deleted.]

3.1.11
cybersecurity
preservation of confidentiality, integrity and availability of information in the cyberspace

Note 1 to entry: The objective is to reduce the risk of causing personal injury or endangering public health, losing public or consumer confidence, disclosing sensitive assets, failing to protect business assets or failing to comply with regulations. These concepts are applied to any system in the production process and include both stand-alone and networked components. Communications between systems may be either through internal messaging or by any human or machine interfaces that authenticate, operate, control, or exchange data with any of these control systems. Cybersecurity includes the concepts of identification, authentication, accountability, authorization, availability, and privacy.

[SOURCE: ISO/IEC 27032:2012, 4.20, modified – Notes replaced with the Note to entry.]

3.1.12
data integrity
property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner

Note 1 to entry: This term deals with constancy of and confidence in data values, not with the information that the values represent or the trustworthiness of the source of the values.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.38]

3.1.13
defence in depth
provision of multiple security protections, especially in layers, with the intent to delay if not prevent an attack

Note 1 to entry: Defence in depth implies layers of security and detection, even on single systems, and provides the following features:

– attackers are faced with breaking through or bypassing each layer without being detected;

– a flaw in one layer can be mitigated by capabilities in other layers;

– a system security becomes a set of layers within the overall network security.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.40]

3.1.14
system integrity
property that a system performs its intended function in an unimpaired manner, free from deliberate or accidental unauthorized manipulation

[SOURCE: ISO/TR 11633-2:2009, 2.14, modified – "of the system" deleted.]

3.1.15
denial of service
prevention of authorized access to resources or the delaying of time-critical operations

[SOURCE: ISO 7498-2:1989, 3.3.25]

3.1.16
hazardous situation
circumstance in which people, property or the environment is/are exposed to one or more hazards

[SOURCE: ISO/IEC Guide 51:2014, 3.4]

3.1.17
security audit
independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures

[SOURCE: IEC TS 62443-1-1:2009, 3.2.101]

3.1.18
security related main function
<of switchgear and controlgear> function of switchgear and controlgear whose failure can result in its unwanted operation which can lead to hazardous situations, in the loss or the corruption of its protective function, or in the loss or the corruption of an extended functionality defined by the manufacturer

Note 1 to entry: When an additonal function such as energy monitoring of a circuit-breaker can be subject to attack leading to the corruption of the security related main function, such as the short-circuit protection, this additional function is considered as a secuity related main function.

3.1.19
threat
potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm

[SOURCE: IEC TS 62443-1-1:2009, 3.2.125]

3.1.20
security policy
set of rules that specify or regulate how a system or organization provides security services to protect its assets

[SOURCE: IEC TS 62443-1-1:2009, 3.2.112]

3.1.21
security vulnerability
weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat

[SOURCE: ISO/IEC TR 24772:2013, 3.1.5.3]

3.1.22
security risk assessment
process that systematically identifies potential vulnerabilities to valuable system resources and threats to those resources, quantifies loss exposures and consequences based on probability of occurrence, and (optionally) recommends how to allocate resources to countermeasures to minimize the exposure

[SOURCE: IEC TS 62443-1-1:2009, 3.2.88, modified – "total exposure" replaced by "the exposure" and notes deleted.]

3.1.23
smart manufacturing
domain of integrated products, processes and resources (cyber, physical, human) to create and deliver products and services, which also collaborates with other domains within an enterprise's value chains and continuously improves its performance aspects

Note 1 to entry: Performance aspects include agility, efficiency, safety, security, sustainability or any other performance indicators identified by the enterprise.

Note 2 to entry: In addition to manufacturing, other enterprise domains can include engineering, logistics, marketing, procurement, sales or any other domains identified by the enterprise.

3.2 Abbreviated terms

APN	access point name
BMS	building management systems
BT	Bluetooth® [1]
CCTV	closed circuit television
CF	communication functionalities
CVSS	common vulnerability scoring system
CRL	certificate revocation list
DNP	distributed network protocol
DMZ	demilitarized zone
DoS	denial of service
DDoS	distributed denial of service
EMC	electromagnetic compatibility
ERP	enterprise resource planning
HMI	human machine interface
HVAC	heating, ventilation, and air conditioning
ICS	industrial control system
IDS	intrusion detection system
IPS	intrusion prevention system

[1] Bluetooth® trademark is an example of a suitable communication protocol available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of this communication protocol.

IT	information technology
IoT	Internet of things
JTAG	debugging interface "Joint Test Action Group" according to IEEE 1149 (all parts)
LAN	local area network
MAC	media access control
MLP	multiprotocol label switching
NFC	near field communication
OT	operational technology
PLC	programmable logic controller
P2P	peer to peer connection
RBAC	role based access control
RS485	recommended standard 485 (according to TIA 485-A)
SCADA	supervisory control and data acquisition
SD card	secure digital card
SSL	secure socket layer
ULP	universal logic plug
USB	universal serial bus
VPN	virtual private network
WCI	wireless communication interface
WLAN	wide local area network

4 General

The integrity or the availability of the main functions of switchgear and controlgear may depend on physical security and cybersecurity aspects. The existing procedures for physically accessing equipment shall be considered as part of the security countermeasures together with the cybersecurity countermeasures.

5 Security objectives

In the context of electrical distribution with switchgear and machine control with controlgear (see Annex A), the overall security objectives are to ensure they operate as designed and configured and specially to avoid unintended operation and to protect its security related main functions.

The main security aspects to be considered are: data integrity, authenticity and availability. They should be detailed in terms of what needs to be protected and how this can be achieved. See Annex C for an overview of the relevant security aspects to be considered and Clause A.3 for security levels.

6 Security lifecycle management

6.1 General

The protections against security attacks should be determined based on the results of a risk assessment in order to identify the potential threats and vulnerabilities, and to define the countermeasures in a document called security requirements specification. It should cover each phase of the life cycle of the equipment and the relevant stakeholders, and it should take into account its physical access and the limits of its environmental conditions (see Figure 1 as an example).

Typical threats and their associated countermeasures are given in the use cases described in Annex B, as listed below in Table 1.

Table 1 – Typical threats

Threat	Use case number
Malicious firmware upgrade	UC1, see Clause B.2 UC5, see Clause B.6
Distributed denial of service attack	UC3, see Clause B.4
Unauthorized access to the production network (OT)	UC2, see Clause B.3
Unauthorized access to the electrical installation	UC4, see Clause B.5
Unauthorized access to the device	UC6, see Clause B.7 UC7, see Clause B.8 UC8, see Clause B.9

The risk associated with corrupting certain security related main functions in some industries may be so severe that efforts associated with risk mitigation may outweigh the benefit of utilizing programmable digital products and highly integrated systems. In such cases, a risk analysis detailing the benefits and drawbacks of utilizing such products and systems is recommended.

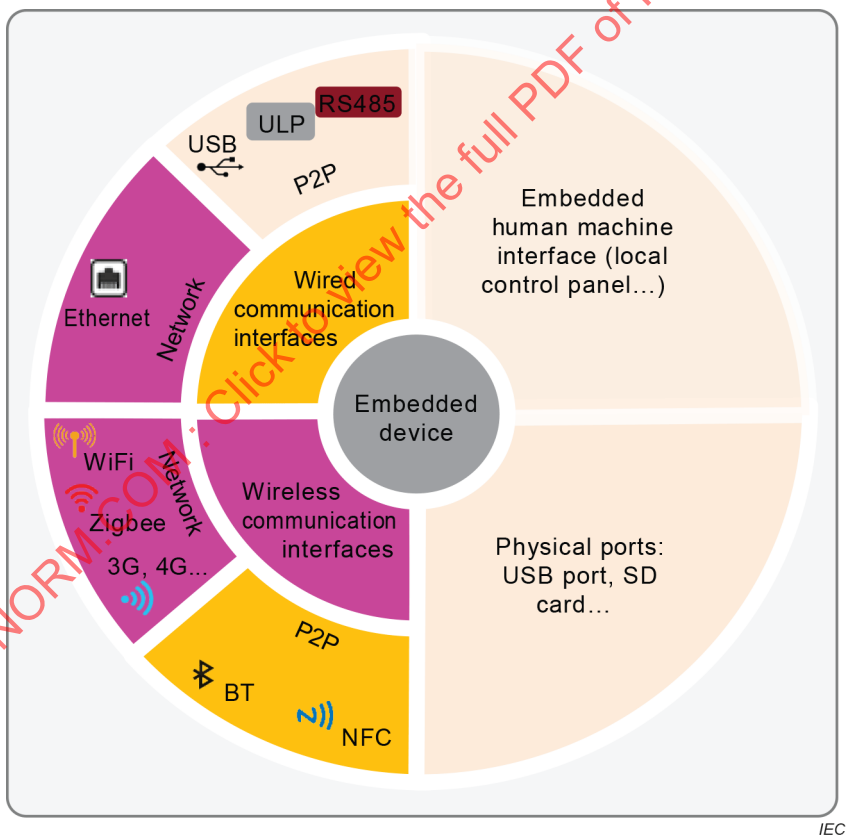


Figure 1 – Example of physical interfaces of an embedded device in an equipment which can be subject to an attack

6.2 Security risk assessment

In general, a security risk assessment is based on a product/system in its environment on which threats and known vulnerabilities are taken into account. After being performed, this assessment will allow defining relevant countermeasures to fulfil the overall security objectives.

All relevant threats and known product/system vulnerabilities possibly affecting the main functions of equipment shall be considered and documented as part of the security risk assessment.

The following aspects should be considered in the risk assessment in combination with the targeted security level:

– correct flow of categorized information throughout the system;
– trust boundaries;
– processes;
– data stores;
– interacting external entities;
– internal and external communication protocols implemented in the product;
– externally accessible physical ports including debug ports;
– circuit board connections such as JTAG connections or debug headers which might be used to attack the hardware;
– potential attack vectors including attacks on the hardware if applicable;
– potential threats, their likelihood, and their severity and consequences as defined by a vulnerability scoring system (e.g. CVSS);
– mitigations and/or dispositions for each threat;
– security-related issues identified;
– external dependencies in the form of drivers or third-party applications (code that is not developed by the supplier) that are linked into the application.

NOTE This list is derived from IEC 62443-4-1:2018.

A vulnerability assessment shall be carried out to identify vulnerabilities, to which identified threats are exploitable, of the equipment within its intended use and the potential influence related to its security related main functions.

The risk assessment shall result in the description of:

– the devices/system covered by a security risk assessment (e.g. mobile control panel);
– the various phases such as design, implementation, commissioning, operation, and maintenance;
– the identified vulnerabilities that could be exploited by threats and result in security risks (including intentional attacks on the hardware, application programmes and related software, as well as unintended events resulting from human error);
– the potential consequences resulting from the security risks, by considering the possibility under which condition these can occur;
– for each phase, the requirements for additional countermeasures;
– the information on the countermeasures taken to reduce or remove the threats.

6.3 Response to security risk

Responses to security risks include the following:

– mitigate intolerable security risks by:
  a) designing the security risk out (avoid); or
  b) limiting the security risk; or
  c) transferring or sharing the security risk (to another entity);
– accept the security risk if tolerable.

6.4 Security requirement specification

Based on the results of the security risk assessment including the vulnerabilities of the equipment, a security requirements specification shall be generated with at least the following:

– the description of the security related main function of the equipment;
– vulnerabilities that can have an impact on this function and assumed threats, if applicable;
– consequences on the security related main function;
– description of proposed security countermeasure(s).

6.5 Important data

Special care should be taken to protect the important data. The important data for the integrity and the availability of the main functions of switchgear and controlgear are the following:

– operating data related to hazardous operation (electrical interlocking, motor starting, reclosing, etc);
– product configuration data, including:
  • circuit-breaker overcurrent protection settings (product ratings, number of poles, etc);
  • proximity sensor settings (sensing range, normally open or normally close output position, etc).

Other data related to the security related main functions of the equipment may also be identified.

Metering function may be sensitive for some businesses. In such case, additional confidentiality measures should be taken.

6.6 System architecture

6.6.1 Control system

Typically, low voltage switchgear and controlgear are installed within assemblies. When needed, communication interfaces are implemented (e.g. gateway) to give remote access for monitoring and control. This can be called a control system.

The attack surface of an attack to a control system is largely a function of its architecture. To assess the architecture-related risks, its level of functionality and its external connectivity should be evaluated.

6.6.2 Levels of communication functionalities

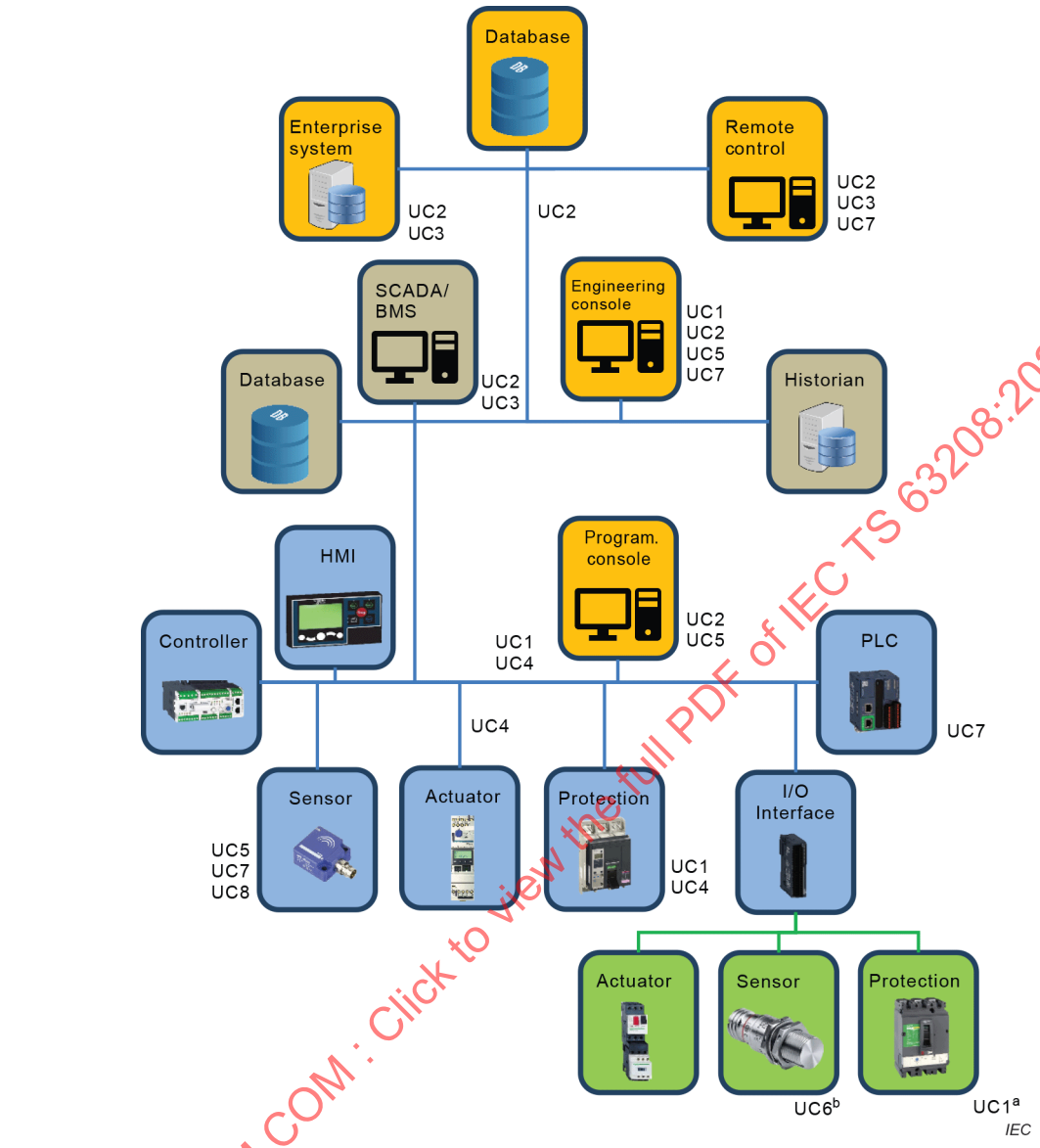
The level of communication functionalities (CF) of the control system can be classified into three levels:

– CF1: minimal systems including sensors, protective devices, programmable logics, HMIs and actuators excluding programming consoles. Point to point communication links may be considered as "CF1-" with limited functionality and limited zone;
– CF2: complex systems with supervisory control and data acquisition (SCADA) or building management systems (BMS), including databases but excluding programming consoles and engineering workstations;
– CF3: very complex system with permanently-connected programming consoles or engineering workstations and other enterprise systems with remote control systems.

Distributed control systems with or without engineering console are considered as CF3.

NOTE Special attention is on programming consoles and engineering stations, which provide significant additional tools to an attacker. Their permanent presence in the control system is sufficient to justify a maximum level. This classification is derived from a publication of ANSSI, the French Network and Security Agency.

Figure 2 illustrate these levels of functionality in a control system architecture.



Key

UC use case number from Annex B

[a] local console communication port access

[b] local HMI access

communication links (wired or wireless)

control wires

non-communicating devices

CF1

CF2

CF3

Figure 2 – Control system architecture with switchgear and controlgear

6.6.3 Levels of connectivity

The connectivity (Cx) of a control system can be classified by the following categories:

– C1: isolated. The whole control system network is completely closed.

– C2: connected to the information system of the enterprise but without permitting operations from outside this information system. The information system can be connected to a public network such as the Internet or even distributed across multiple sites.

– C3: connectivity C2 using wireless communication as depicted in Figure 3. The wireless access gives more vulnerabilities to attacks.

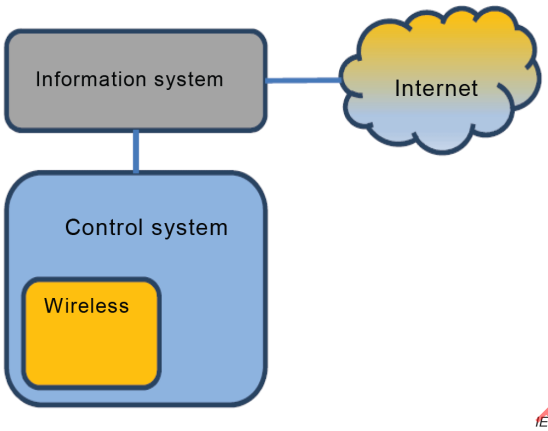


Figure 3 – Control system connectivity level C3

– C4: distributed control system permitting operations from outside as depicted in Figure 4. Different sites communicate with each other via a private infrastructure. This may be completely private or leased from a telecommunications operator. This category also concerns control systems that permit operations from outside the site or from a management network (e.g. remote maintenance, remote management).

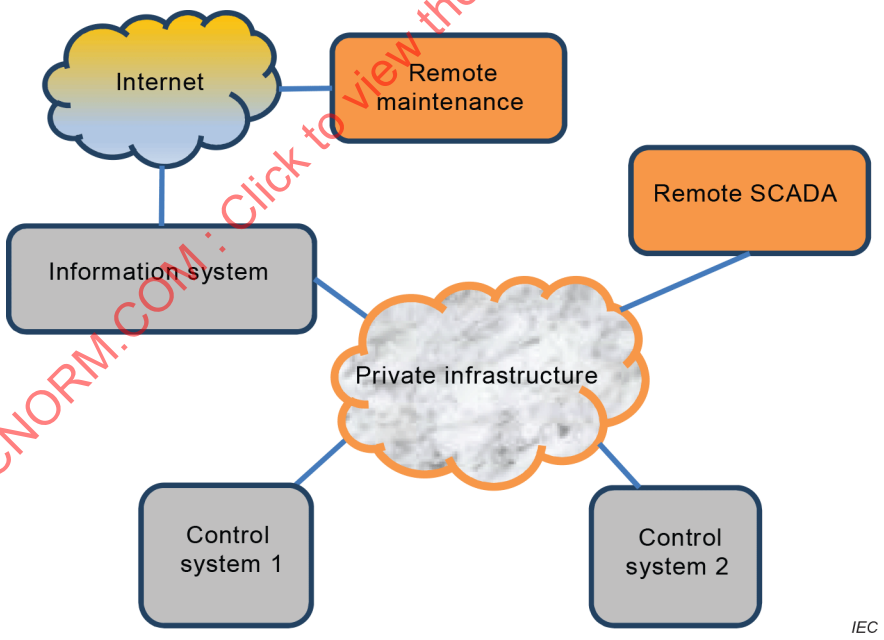


Figure 4 – Control system connectivity level C4

– C5: distributed control system with public infrastructure (Internet) as depicted in Figure 5. An attacker can easily reach various access points of the control system. This obliges the implementation of additional countermeasures. Moreover, no resources are dedicated to the control system, which can become a "collateral victim" of abnormally high network utilization.

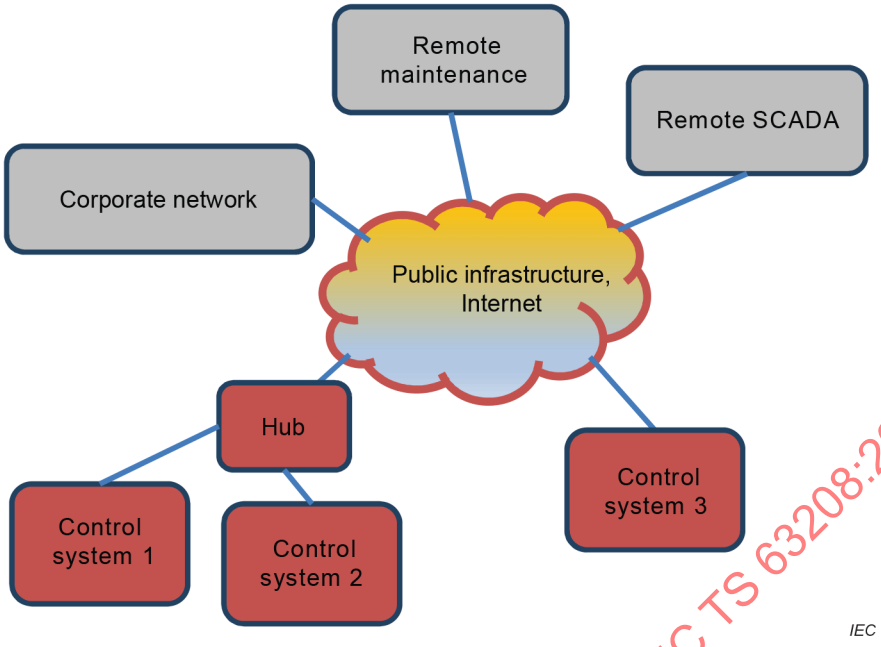


Figure 5 – Control system connectivity level C5

Infrastructure such as private access point name (APN) or virtual private network (VPN) of type multiprotocol label switching (MLP) falls into this category.

In this category, new potential vulnerabilities related to the presence of an infrastructure are very difficult – or even impossible – to monitor and control in their entirety, in particular from the perspective of physical access. All vulnerabilities related to remote maintenance are also present.

6.6.4 Control system exposure levels

The exposure of the control system is a combination of its levels of communication functionality and connectivity. Table 2 gives a level of exposure from E1 (least exposed) to E5 (most exposed). This indicates the amount of risk that can be introduced into the control system. A higher risk will require a more extensive risk assessment.

Table 2 – Level of exposure of a control system

Functionality/Connectivity	C1	C2	C3	C4	C5
CF3	E3	E3	E4	E4	E5
CF2	E2	E2	E3	E4	E5
CF1	E1	E2	E3	E4	E5
Key E1 least exposed E5 most exposed					

The levels of functionality and connectivity do not vary independently. Therefore, some cells may not correspond to any real control system. Other factors can influence the levels, including the number of devices involved, and the heterogeneity of the devices used should be considered in the risk assessment.

Examples of risk assessment associated with their level of exposure are under consideration.

Non-communicating devices illustrated in green in Figure 2 are not considered in the levels of exposure, but shall be covered in the whole risk assessment when they include embedded software.

The level of exposure is used for evaluating the severity of the exposure of the equipment to attacks in order to select the appropriate countermeasure. See Annex B.

7 Security requirements

7.1 General

The following requirements are based on the typical use cases of Annex B.

Following the approach of Clause 6, the manufacturer shall implement the relevant security countermeasures given in the following subclauses 7.2, 7.3 and 7.4.

The communication accessories associated with switchgear and controlgear are assumed to maintain their functional integrity level within the intended industrial environment (physical and EMC).

NOTE Powerful, with extended connectivity and inexpensive consumer off-the-shelf communication devices, are often not appropriate for industrial environments and give too many opportunities for cyber-attack.

7.2 Cybersecurity aspects

Cybersecurity aspects are partly derived from IEC 62443-4-2:2019.

If applicable, as minimum requirements, the identification and authentication, use control, system integrity and resource availability shall be taken into account. Data confidentiality, restricted data flow and timely response to events may be relevant in certain cases but are not required in this document.

Consequently, the minimum required security profile is depicted in Figure 6. The details of the requirements belonging to each security aspect are under consideration for inclusion in Annex C.

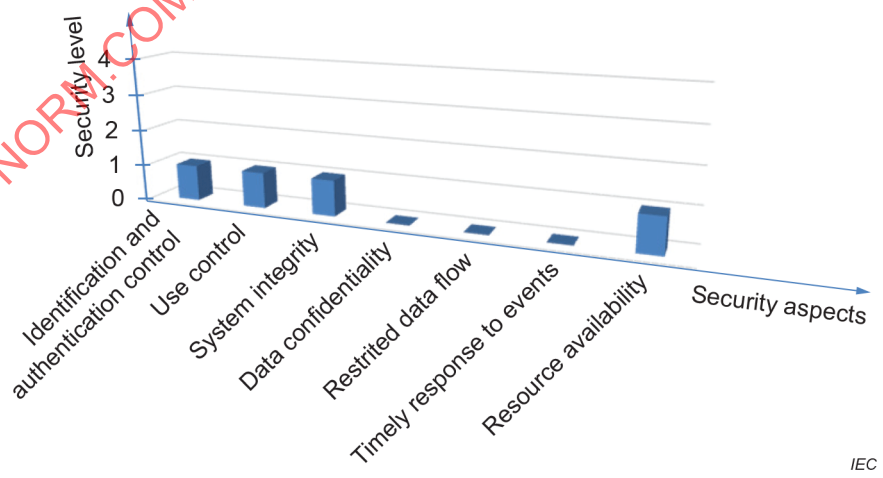


Figure 6 – Switchgear and controlgear minimum security profile

Annex C provides information about each cybersecurity aspect.

The appropriate security level vectors shall be selected according to the results of the risk assessment according to Clause 6.

7.3 Physical access and environment

According to IEC 60364-7-729, restricted access areas with switchgear and controlgear assemblies shall not provide access to unauthorized persons. In addition, door(s) provided for closed restricted access areas shall allow easy evacuation to the outside by opening without the use of a key, tool or any other device not part of the opening mechanism.

NOTE In North America, requirement for physical security of critical operations power systems are given in Clause 708.5 of NFPA 730, Guide for Premises Security.

Based on the results of the risk assessment, a strategy for providing physical security when appropriate shall be developed, documented, and implemented.

Electrical circuits and equipment for critical operations power systems shall be accessible to qualified personnel only.

Typical measures for managing the physical access to switchgear and controlgear are locked doors of technical rooms and individual distribution and control switchboards, sealed panels, alarm systems and video monitoring.

According to A.11 of ISO/IEC 27001:2013, several requirements are derived to premises where low voltage switchgear and controlgear assemblies are installed. Appropriate user instructions shall be given for addressing the following requirements.

a) For secured areas in order to prevent unauthorized physical access, damage and interference to the security related main functions of the equipment:
   1) Physical security perimeters should be defined and used to protect areas that contain equipment supporting security related main functions.
   2) Physical entry controls: access control should be defined and implemented to authorized persons for entering premises where switchgear and controlgear are accessible such as electrical restricted access areas.
   3) Detective and reactive physical security monitoring: security means should be deployed to monitor premises security. For example, CCTV should be used to view and record access to sensitive areas within an organization's premises, guards should be deployed to detect intruder access to an organization's premises, or burglar alarms and other devices should be used to detect the presence of intruders within an organization's premises.
   4) Protecting against external and environmental attacks: physical protection against natural disasters, physical attack or accidents should be considered, and if appropriate should be designed and implemented.
b) For equipment in order to prevent loss, damage, theft or corruption of equipment and interruption to the organization's operations:
   1) Equipment siting and protection: storage facilities should be secured to avoid unauthorized access. Controls should be adopted to minimize the risk of potential physical and environmental threats, for example theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, higher EMC disturbance levels than the generic levels given for the relevant EMC environment and vandalism.
   2) Cabling security: power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference or damage.
   3) Equipment maintenance: equipment should be correctly maintained to ensure its continued availability and integrity. For example, firmware should be updated according to the manufacturer's notice.

c) Equipment tampering: when the above countermeasures are not implemented, the equipment should be secured to avoid internal access, for example: disable/remove JTAG ports, apply tamper evident seals to removable housings, disable unused processor peripheral ports, design features in device housings to make them tamper resistant, utilize tamper resistant hardware to join component housing sections, where local setting controls are supplied (dials or dip switches), provide means of locking or sealing them from tampering.

7.4 Equipment requirement

7.4.1 General

The manufacturer of the equipment shall consider the requirements of 7.4.2 to 7.4.8.

7.4.2 Hardening

Only software/services that are needed to support the main functions of the product shall be implemented in the product. For instance, services for debugging purposes used during development should be removed before release.

To limit backdoor accounts and avoid hardcoded credentials, product should not have any accounts, passwords or private keys that cannot be changed, disabled or removed by an authorized end-user.

7.4.3 Encryption techniques

Accepted industry recommendations and guidelines such as algorithms according to IEC and/or ISO standards shall be used. Product manufacturers should neither invent their own algorithms nor use algorithms from unknown sources. The providing source should guarantee updates and patches in case of vulnerabilities and failures.

The manufacturer should establish a vulnerability monitoring for the utilized security functionalities.

EXAMPLE Integration of open SSL (secure socket layer).

7.4.4 Embedded software robustness and integrity

7.4.4.1 Security quality

Security quality checks should be performed for example with robustness testing, vulnerability scanning, static code analysis or binary code analysis. This is often done using available tools on the market.

NOTE Guidance for the development of embedded software for switchgear and controlgear including secure coding is described in IEC TR 63201.

7.4.4.2 Software integrity and authenticity

Software deliverables shall be digitally signed in such a way as to allow customers to verify integrity and authenticity of software before using it.

The digital signature should be checked by the user before installation on the device.

The digital signature should be ultimately verified by the device before accepting the installation. Both secure boot and secure upgrade should be implemented. This verification shall be done in case of software upgrade from remote or wireless communication.

Asymmetric algorithms used for signature shall be selected from FIPS 186-4 or any other recognized standards.

Digital signature shall be formatted using well known standards. IEC TS 62351-6 recommends using X.509 format, for example.

Manufacturers shall build a process to protect the private key used for signature from unauthorized access (see examples of how to manage keys in IEC 62351-9). In case of compromise of the private key, like disclosure or abusive use, manufacturers shall take adequate measures to restore the integrity of the embedded software and to revoke all certificates associated to the key. A certificate revocation list (CRL) shall be kept available and updated periodically by the manufacturer.

7.4.5 Denial of service

DoS and DDoS attacks may cause:

– flooding (saturation) of communication network. In this case, switchgear and controlgear are no longer available and cannot send data and alarms, or execute SCADA or controller commands;

– overloading of equipment resources which makes main functions inoperative or behaving improperly;

– reset of the equipment which makes main functions inoperative for some time.

Embedded software of switchgear and controlgear shall be designed in a way to prevent impact of DoS and DDoS type attacks on the main functions of switchgear and controlgear. Only required services and ports shall be implemented to reduce the exposure to attack. In addition, a mechanism limiting the data rate can be implemented by dropping data packets when a rate threshold is reached.

System architecture shall be designed in a way to lower the probability and the impact of DoS or DDoS. For example, OT network shall be separated from IT network and switchgear and controlgear shall not be exposed directly to the Internet without appropriate countermeasure.

NOTE See IEC 62443-3-2[2] for details.

7.4.6 Authentication of users

When interfaces of switchgear and controlgear are intended to be accessible to the user on the front door of the equipment or remotely, they shall provide means to identify and authenticate legitimate human users interacting with them.

Role based access control (RBAC) techniques should be used to implement authentication and authorization mechanisms. Authentication of users could be achieved for example using passwords, smartcards, biometric data, etc. IEC 62351-8[3] may be used for this purpose.

Users authorization shall be granted (permissions) in relation to their roles and permissions. Least privilege principle should be considered for the definition of roles and permissions.

For first use, switchgear and controlgear shall provide at least one default credential, which shall be modified.

A security policy should be applied to strengthen the authentication process over time. Switchgear and controlgear should support implementation of such policy.

The authentication could be performed within the equipment itself or by a system component on the OT/IT network.

---

2 Under preparation. Stage at the time of publication: IEC RFDIS 62443-3-2:2020.

3 Under preparation. Stage at the time of publication: IEC CFDIS 62351-8:2020.

Security related events like login attempts should be logged at equipment level or at system level for monitoring or later analysis. In addition, this event storing (audit log) should be protected from tampering (integrity protection).

Authentication and authorization of machine users should be considered to make sure that commands and data are from a trusted equipment.

7.4.7 Communication systems

Unsecured communication systems shall be either isolated from outside the protected perimeter via a physical access measure or using a firewall at the system level or other equivalent countermeasures such as VPN or IPsec.

When authorization (which can include encryption) and authentication are required, secured communication protocols shall be considered, for example: Secure Modbus, "secure" ProfiNet[4] under consideration, IEC TS 62351-5 as secured extension for DNP3 or IEC 60870-5 communication protocols, as well as IEC TS 62351-6 for IEC 61850 communication protocols.

7.4.8 Wireless communication

For securing wireless communication, the state-of-the-art recommendations shall be followed, for example NIST 800-121 about Bluetooth or other recognized standard.

8 Instructions for installation, operation and maintenance

In addition to 6.3 of IEC 60947-1:2020 (Instructions for installation, operation and maintenance), the manufacturer shall provide all information for installing products and for configuring security controls needed to maintain the intended security level.

The manufacturer shall specify the countermeasures to be taken about the potential security threats related to the security related main functions of the equipment.

The following information should be included in product documentation:

– physical security requirements, if required;

  EXAMPLE 1 Product is in a locked cabinet because it has a non-protected externally accessible communication port.

– descriptions of communication ports and services;

– dependencies on other system components for secure deployment;

  EXAMPLE 2 An IO-Link sensor depends on the IO-Link master to ensure restrictions on protected mode behaviours as well as authentication of configuration.

– description of all user and system accounts with recommendation to change default passwords;

– deployment guidelines;

– specific instruction on how to configure security controls provided either by the product or in addition to the product (for instance firewall, antivirus); guidance for setting up event logging and alerts. See Annex D.

For relevant potential security requirements and recommendations, the manufacturer should provide security signs, graphical symbols or security notes of the vulnerability. The symbol shown in Figure 7 (IEC 60417-5569:2005-08 combined with ISO 7000-2410:2004-01) should be used in the documents to identify security instructions.

---

4 ProfiNet® trademark is an example of a suitable communication protocol available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of this communication protocol.

Figure 7 – Example of security instruction symbol

The effectiveness of the cybersecurity countermeasures of the equipment will depend on the risk analysis and the consequential cybersecurity strategy of the whole system to be implemented and managed. Reference to IEC 62443-2-1 or ISO/IEC 27001, as appropriate, can be given in the documentation of the equipment as a general best practice standard for this purpose.

Security vulnerabilities experienced in the field shall be shared with the relevant parties and recommendations shall be provided about the associated risks and actions. For this purpose, Clause 10 of IEC 62443-4-1:2018 or A.10 of ISO/IEC 27001:2013, as appropriate, applies.

Guidance for the attention of the user on how to deploy an appropriate cybersecurity strategy necessary for taking the benefits of the countermeasures embedded in the equipment are developed in Annex D.

9 Development and testing

9.1 General development method

To verify that all security requirements have been implemented according to the product security requirements, the development and testing shall follow a well-defined and managed process. A secure development plan shall be defined with the following:

a) Specification of the implementation of security features in relation to the security requirements defined in Clause 6 of IEC 62443-4-1:2018 shall be applied when applicable to switchgear and controlgear.

b) Subclause 7.5 of IEC 62443-4-2:2019 (Security functionality verification) and 10.1 of ISO/IEC 27001 shall be considered for the capability to support verification of the intended operation of security functions.

c) Software management plan according to Clause 5 of IEC TR 63201:2019 applies with the security countermeasures considered as main functions. The following additional security management requirements from Clause 5 of IEC 62443-4-1:2018 apply:

   – security of the development environment, secure repositories and security in the version control (5.9 of IEC 62443-4-1:2018);
   – security checkpoints within the project milestones (5.2 of IEC 62443-4-1:2018);
   – developers' capability of avoiding, finding and fixing vulnerabilities (5.6 of IEC 62443-4-1:2018).

d) The design lifecycle shall follow Clause 7 of IEC TR 63201:2019 and, in particular, the secure coding principles.

Further conformance tests for power system equipment can be found in IEC 62351-100 (all parts).

9.2 Testing

Security verification and validation testing should be carried out during the design lifecycle. Clause 9 of IEC 62443-4-1:2018 applies.

NOTE Complementary testing methods can be found in UL 2900-1.

Annex A
(informative)

Cybersecurity and electrical system architecture

A.1 General

An efficient way to mitigate the security risk is to distribute countermeasures at the different levels of the architecture of the considered system. Switchboards and control boards are also used at different levels of the electrical distribution and of the power control system.

A top-down approach should be followed to identify the appropriate security countermeasures at each layer of the architecture of the electrical system.

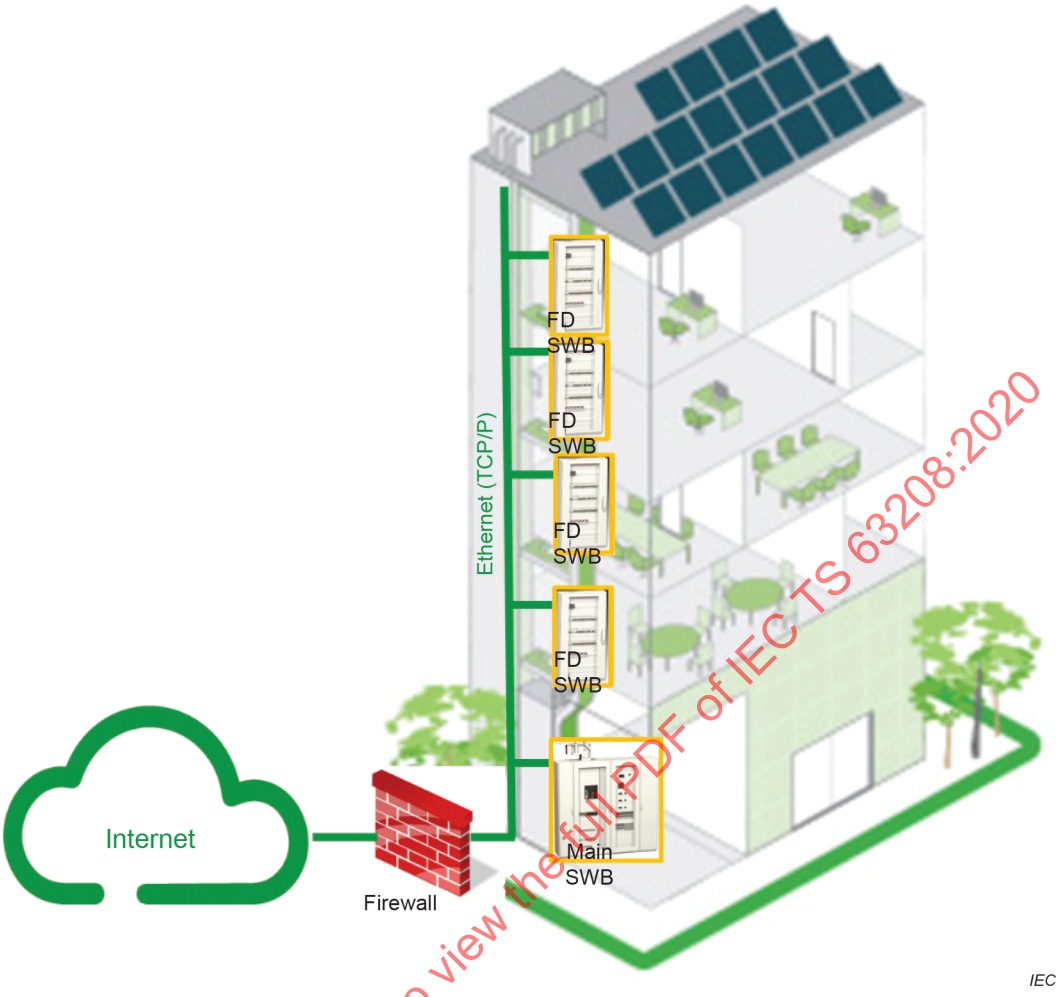
A.2 Typical architecture involving switchgear and controlgear and their assembly

A.2.1 Building

The security layers of a building can be defined as follows:

1) site (campus) network: firewall, anti-virus, VPN;
2) IT Services (ERP, e-mail server, office IT, etc.);
3) building networks: intrusion detection, network interfaces (HVAC, IT, BMS, etc.);
4) technical room: guards, locks, access control;
5) switchboard communication network or system: panel firewall, authentication, security audit;
6) panel programmable controller: application hardening, patch management;
7) switchgear product communication: control, configuration.

Figure A.1 shows an example of a building electrical architecture.



Key

FD SWB	final distribution switchboard
Main SWB	main switchboard

Figure A.1 – Building electrical architecture

A.2.2 Manufacturing

The security layers of a manufacturing facility can be defined as follows:

1) IT network: firewall, VPN, DMZ;
2) manufacturing network: firewall, VPN;
3) workshop network: intrusion detection;
4) physical: locks, access control;
5) machine communication network or system: machine firewall, authentication, anti-virus, security audit;
6) machine controller: application hardening, patch management;
7) safety control system: safety integrity;
8) controlgear communication: control, configuration, safety integrity.

Figure A.2 shows four typical manufacture plants i.e. car production and machine tool, conveyor technique and packaging, chemical industry and food industry.

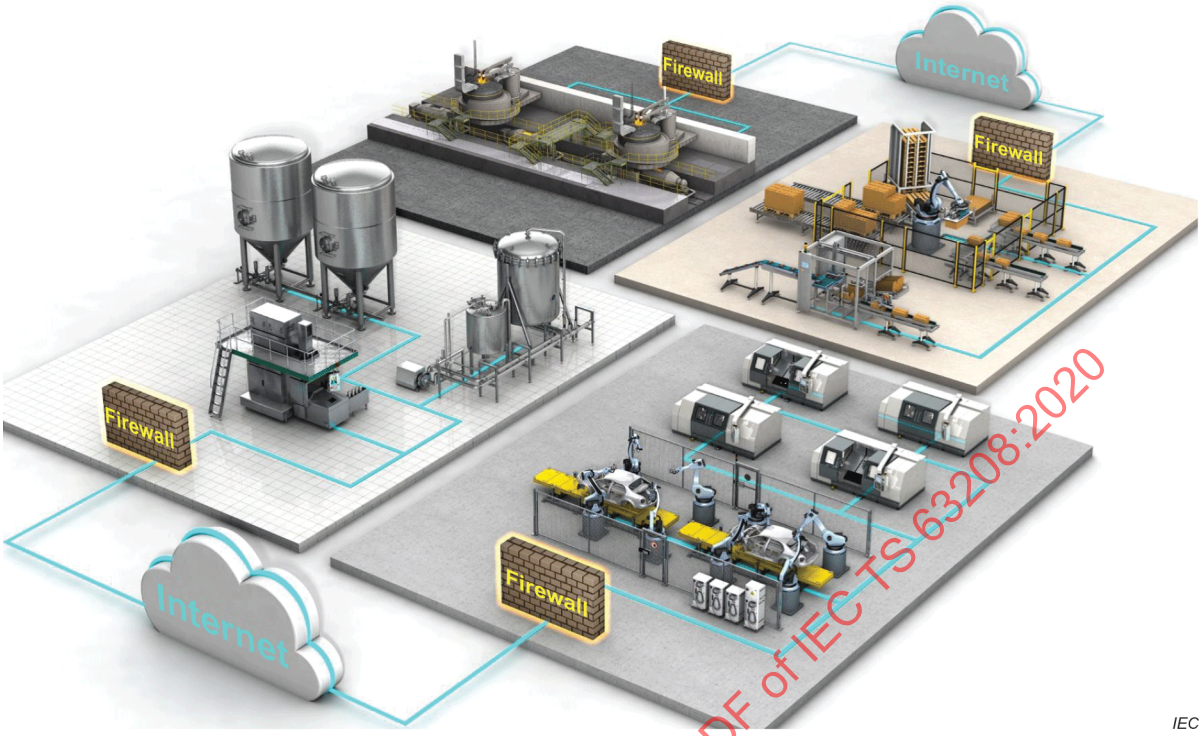


Figure A.2 – Industrial plants

A.3 Security levels and product standards

When a product standard addresses security risks in interfaces of electrical devices, for example fieldbus, USB, LAN or remote-control operation, devices and subsequent communication layers, a qualitative approach addressing security should be determined and classified in one of the following security levels derived from IEC 62443-4-2:

a) SL-1: protection against casual or coincidental violation;

b) SL-2: protection against intentional violation using simple means with low resources, generic skills and low motivation;

c) SL-3: protection against intentional violation using sophisticated means with moderate resources, specific skills related to the considered equipment and moderate motivation;

d) SL-4: protection against intentional violation using sophisticated means with extended resources, specific skills related to the considered equipment and high motivation.

Product standard should specify the security requirements which are needed to achieve the security levels mentioned in a) to d) while considering the following aspects:

1) countermeasures for protection against a given type of threat by configuration during the design and installation phase;

2) based on a risk assessment, the need to protect the particular zone against the relevant level of threat (see a) to d));

3) how the asset owner, system integrator, product supplier and/or any combination of these shall configure the zone, system or component to meet the particular security requirements described in a) to d).

Annex B
(informative)

Use case studies

B.1 General

Annex B describes the typical use cases which are used to justify the relevant requirements applicable for switchgear and controlgear and their assemblies. The format of the description follows IEC 62559-2:2015.

B.2 Use case 1 – Protection against malicious firmware upgrade of a circuit-breaker

Name of use case	Protection against malicious firmware upgrade of a circuit-breaker.	
Lifecycle	Electrical installation lifecycle of a building, industrial/commercial site or an LV utility sector with a minimum level exposure E3 (CF3, C2) according to Table 2.	
Phase	Commissioning and maintenance.	
Objective and benefit for whom	To ensure continuity of energy supply to end-user, facility manager, especially during extensive use of the occupancy or load duty. To protect the related critical data (see 6.5).	
Actors	Hacker	Attacker who manages the cyber-attack.
	Field facility manager	Manager checks the access to the network and ensures the correct countermeasures are taken.
General description: which actor does what	Hacker has managed in his laboratory to build a corrupted firmware (including a logical bomb). Hacker sends a fake e-mail (spam) from the manufacturer to a list of sites facility managers with the malicious firmware attached asking the customer to make an upgrade due to a serious bug on the circuit-breaker. A facility manager trusts the e-mail and proceeds to the upgrade. The corrupted firmware is operational like the original one. At a predefined date the circuit-breaker opens (logic bomb activated). All infected circuit-breakers open at the same time. Facility manager does not see any root cause of the event. Each time he closes the circuit-breaker, it opens again. Immediate impact on production or building operation. Facility manager contacts manufacturer for diagnosis and correction. All provided data to the support are compliant with the expected behaviour (original firmware). Option: hacker may ask for ransom.	

Detail description: trigger, steps relating to how actors are working together, etc.		
Countermeasures	Manufacturer	To ensure the integrity and the authenticity of the firmware, all circuit-breakers firmware versions should be digitally signed by the manufacturer. This digital signature should be verified before allowing execution.
	Facility manager	Facility managers should define rigorous firmware update policy. For example: – defining the list of people in charge of the critical maintenance activities such as firmware updates; – defining the needed cybersecurity relevant training(s); – defining for these people the relevant access rights with the approved updating tools (computer, software, etc); – verifying the website of the manufacturer to get the last up-to-date cybersecurity countermeasures.

B.3 Use case 2 – Protection against unauthorized access to electrical production network

This cyber-attack use case is based on a real case as described in the following link (https://www.wired.com/2015/01/german-steel-mill-hack-destruction/).

Name of use case	Protection against unauthorized access to production network. In case of unauthorized access to the production network, attackers can shut down and/or send improper commands to physical devices (i.e. circuit-breakers).	
Lifecycle	Electrical installation lifecycle in a plant or a factory with a minimum level exposure E2 (CF1, C2) according to Table 2.	
Phase	Active phase of the plant.	
Objective and benefit for whom	To ensure the inviolability of the production network in order to avoid improper commands and modifications of the state of the physical devices installed. Avoid critical accidents and improper unsafe use of the devices.	
Actors	Hacker	Attacker who tries to enter the production network.
	Field facility manager	Actor who checks the access to the network and ensures the correct countermeasures are taken.
	Security manager of IT department	Responsible for the awareness of possible phishing e-mails and responsible for the effectiveness of the firewall and for the safety of the network.
	Employees	Employees do not recognize the phishing attack and click a link to a malicious site, granting the attacker access to the company network.
General description: which actor does what	Hacker wants access to the production network. Exploiting the connection between the company network (IT) and the production network (OT), he starts to send phishing e-mails (to specific targets and trustable contents) to employees, in order to get a login and password to gain access to the network. High know-how of the hacker not only on IT, but also on industrial control system (ICS). Some employees trust the phishing e-mails and the hacker is able to reach the company network and consequently the production network with direct access to the devices. The more substantial the automation of the plant, the bigger the risk of critical damage. Facility manager detects the abnormal behaviour and disconnects automatic control of the devices and decides to start manual operations. IS department starts the investigation in order to understand how the hacker was able to enter the production network and control the physical devices.	

Detail description: trigger, steps relating to how actors are working together, etc.	Phishing e-mails	Trustable and addressed to specific targets.
	No separation of company network and production network	Hacker exploits this weakness of the system.
	Shutdown of the automation	Facility manager interrupts the automatic operation of the system and switches to manual operation.
	Detection and understanding of the origin of the attack	IS and facility manager check accesses and unusual operations inside the network.
Countermeasures	Generally, to apply multiple protection layers called defence in depth principle: – segregation between company network (IT) and production network (OT); – increase employee's awareness about phishing e-mails; – verify the configuration of the firewalls and check their effectiveness; – periodic check of external access to the network; – presence of a backup and recovery process in order to quickly recover after an attack; – remote access to the devices (circuit-breakers) should be protected by an authenticating mechanism (password) or a security level (the password shall be different from the default one and the user shall change it); – manage users by providing appropriate access rights for the different functions (only authorized users can access the physical device → reduction of the success rate of the phishing e-mails).	

B.4 Use case 3 – Protection against DDoS (distributed denial of service) attack through insecure IoT devices

This cyber-attack use case is based on a real case as described in the following link (https://thehackernews.com/2016/11/heating-system-hacked.html).

Name of use case	Protection against DDoS attack through insecure IoT devices. DDoS attack overloading production network with Internet traffic from multiple locations causing control system to fail.	
Lifecycle	Electrical installation with a minimum level exposure E4 (CF2, C4) according to Table 2.	
Phase	Operation of the electrical installation of a building, industrial/commercial site or a low voltage utility sector.	
Objective and benefit for whom	To ensure continuous operation of control system when system is under DDoS cyber-attack. Avoid control system shutdown and malicious communication inside the production network.	
Actors	Hacker	Attacker who launches DDoS attack against vulnerable devices.
	Facility service company	Company in charge of managing building operation and maintenance.
	Field service technician	Manages on site installation including maintenance, repair and customer support.

General description: which actor does what	The hacker installs malware on one insecure IoT device connected to Internet. Examples of insecure devices are consumer electronic devices with unproven security level. Many devices use default password and lack software update mechanism. The malware scans Internet for other insecure IoT devices to infect and tries to login on discovered devices using common usernames and default passwords. The malware is installed on devices where the login is successful. By executing the malware, hundreds or even thousands of insecure IoT devices turn into remotely controlled "bots" ready to contribute to DDoS attacks. The hacker scans Internet for devices to attack and launches a DDoS attack to selected devices utilizing the bots. One of the devices that is the target of the attack is a heating control system that controls heating and ventilation in a building. The heating control system is overloaded by the traffic and tries to respond to the attack by rebooting the main control circuit. This is repeated and finally the control system is shut down, causing unplanned downtime of both heating and ventilation in the building. The facility service company that monitors and adjusts the control system remotely discovers that the remote connection is lost. Connection cannot be re-established, so the facility service company sends out a service technician to the building to investigate the problem locally. The problem is solved in two steps. 1) The first step is taken by the technician who disconnects the affected hardware from Internet and switches the heating system to manual operation. 2) The facility service company checks for the causes and tries to find a solution. The DDoS attack is addressed by installing a firewall between the control system and Internet before taking the system online again. The firewall prevents the DDoS attack to reach the control system, because the malicious traffic is filtered out.
Countermeasures	Apply multiple protection layers according to the defence in depth architecture: – System level – Address security throughout the lifecycle of the control system, from design to installation and commissioning to maintenance. – Network level: • logical separation between control system LAN (local area network) and other network by using firewall, managed switches, unidirectional gateways, etc. Only legitimate traffic should be allowed on control system LAN. • do not connect any consumer device or insecure device (device with weak security) to control system LAN. – Device level – Improve security quality of control system devices by taking the following countermeasures: • disable unused ports and services; • keep the device firmware updated to make sure the latest security patches are installed; • test device robustness, including flooding and fuzzing; • replace default password with strong password that is unique for the specific device.

B.5 Use case 4 – Protection against unauthorized access to the electrical network using illegitimate device

Name of use case	Protection against unauthorized devices connected to the communication network. Capture of information, remote control of switchgear.
Lifecycle	Electrical installation with an initial level of exposure E2 (CF1, C2) according to Table 2. This level is changed to E4 (CF1, C4) after hacking with an additional communication device.
Phase	Operation or maintenance of the electrical installation of a building, industrial/commercial site or a low voltage utility sector.
Objective and benefit for whom	To ensure the protection and the security of a network, exposed to risks due to unauthorized devices integrated into this network. Avoid shutdown and bad communication inside the network.

Actors	Hacker	Attacker who tries to take control of the network remotely.
	Network manager	Actor who works in order to maintain and secure the network at any time, responsible for the IoT devices connectivity.
	Security manager of IT department	Responsible for the effectiveness of the firewall and for the security of the network.
	Field operator	Checks and fixes installed devices.
	Intruder	Attacker who managed to intrude into the electrical room and connect an unauthorized 3G/4G device to the network.
	Site security manager	In charge of the security of the premises.
General description: which actor does what	Because of weak physical security in the electrical rooms and switchboards, an intruder is able to intrude into the electrical room, to open the switchboard and to connect a 3G/4G communication device to the network. Remotely, the hacker is able to connect to the internal network thanks to the 3G/4G communication means and bypass all Internet and intranet networks security countermeasures (firewalls…). He is able to: – send commands to the switchgear for open; – modify data and settings of the switchgear; – send incorrect data to the supervision of the system (if any); – disturb the behaviour of the network. This may have an immediate impact on the correct operation of the system, due to the shutdown of some of the switchgear.	
Detail description: trigger, steps relating to how actors are working together, etc.	**Physical access and use of an illegitimate communication device**	
	Access	Because of a lack of physical security policy and countermeasures, an unauthorized person is able to access electrical rooms and switchboards content. This is a security breach.
	Connection	An intruder is able to connect an illegitimate device with autonomous long-range communication capability (3G/4G or even Wi-Fi).
	Attack	Use of remote connection to inject malicious data and/or behaviours.
	Detection	Local field operator or network manager detects the abnormal behaviour and works to find the root cause. Further physical inspection of field operator detects and dismantles the illegitimate device.
Countermeasures	To define and implement physical security policy and implement illegitimate device detection processes	Apply defence in depth principle by adding physical security: – physical security shall be implemented to prevent unauthorized people from accessing the electrical rooms; – physical security shall be implemented to prevent unauthorized people from accessing the switchboards; – physical inspection should be conducted to detect suspicious components or devices. Monitoring of the network shall be applied to detect new/suspicious communicating devices. – the good answer is enrolment of the system: only devices that have a certificate signed by an authorized authority can communicate within the system.

B.6 Use case 5 – Protection against malicious firmware upgrade of a sensor (e.g. proximity switch), mounted in a machine wired-connected by IO-Link interface

Name of use case	Protection against malicious firmware upgrade of a sensor (e.g. standard proximity switch), mounted in a machine wired-connected by IO-Link interface.	
Lifecycle	Installation, operation, maintenance with a minimum level exposure E2 (CF1, C2) according to Table 2.	
Phase	Operating phase of machinery, regular maintenance update.	
Objective and benefit for whom	To ensure the up-to-date configuration, the integrity of the files (configuration, functions, parameters, etc.) received from the manufacturer. Benefit for operator company, operator and manufacturer of the sensor: reliable function of the machine, no customer complaints.	
Actors	Hacker	Attacker who tries to modify or attack the installed firmware.
	Manufacturing automation manager	He gives the authorizations and roles and he supervises the proper maintenance process of the automation system.
	Service operator	Initiator of the update (doing).
	Field operator	No activity in this process.
General description: which actor does what	Hacker has managed in his laboratory to build a corrupted firmware (including a logical bomb). The hacker presents the corrupted firmware for downloading by e-mail or Internet/fake homepage. The manufacturing automation manager trusts the fake e-mail, Internet/fake homepage (corrupted firmware). The manufacturing automation manager makes the download and stores the corrupted firmware on a maintenance tool. The service operator disconnects the connecting cable or plug of the sensor and connects the sensor to the maintenance tool. The service operator initiates the download of the corrupted firmware from the maintenance tool to the sensor in accordance with the defined process. The service operator disconnects the maintenance tool and connects the connecting cable or plug with the sensor again. The machine is operating, the corrupted firmware is unnoticed until the corrupted firmware causes a malfunction (faked data/information), etc. The manufacturing automation manager or operator notices a malfunction and sends a customer complaint to the manufacturer (the detection of skimming is improbable). The service manager or the manufacturer replaces the sensor at the machine. The quality department of the manufacturer makes investigations to find out the reason for the malfunction. Suitable plausibility or validity check of the installed firmware identify the corrupted firmware.	
Detail description: trigger, steps relating to how actors are working together, etc.	Manufacturing automation manager	Manufacturing automation manager trusts the fake e-mail, Internet/fake homepage. He thinks it is a legitimate data source.
	Service operator	Service operator trusts the corrupted firmware. The maintenance tool and the sensor have no built-in plausibility or validity check for identification of the corrupted firmware.
	Manufacturing automation manager	Manufacturing automation manager or quality department launches a customer complaint.
	Manufacturer	The manufacturer makes analyses to find out the reason for the customer complaint. By comparing the source code and check sum it is possible to find the corrupted firmware.

Countermeasures	Technological	To ensure the integrity and the authenticity of the firmware, all sensors firmware versions should be digitally signed by the manufacturer. This digital signature should be verified before allowing execution. The digital signature shall be defined in relation to the security level (SL-1 to SL-4 of this document) and the potential risk of a malfunction. A risk analysis is necessary. (These aspects will be considered during the maintenance of IEC 60947-5-7:2003).
	Organizational	Manufacturing automation should define rigorous firmware update policy. For example: – defining the list of people in charge of the critical maintenance activities such as firmware updates; – defining the needed cybersecurity relevant training(s); – defining for these people the relevant access rights with the approved updating tools, e.g. computer, software, maintenance tool (from manufacturer); – verifying the website of the manufacturers to get the last up-to-date cybersecurity countermeasures; – defining the allowed source (homepage/links of the manufacturer) for downloads.

B.7 Use case 6 – HMI: human machine interface – Protection against unauthorized access to a simple sensor (mounted in a machine) – improper parametrization

Name of use case	HMI: human machine interface – Protection against unauthorized access to the simple sensor mounted in a machine – improper parametrization.	
Lifecycle	Operation with a minimum level exposure E1 taken from Table 2 as the lowest level even if there is no level of communication functionality in this use case.	
Phase	Active phase of machinery.	
Objective and benefit for whom	To ensure the continuity, validity of information/data and function. Benefit for operator company, operator and manufacturer of the sensor: reliable function of the machine, no customer complaints. This use case describes a simple sensor, provided only with push-buttons and a LED for programming the parametrization.	
Actors	Attacker	Attacker who tries to modify the specified and configured sensor parameter(s) for the application.
	Manufacturing automation manager	No activity.
	Service operator	No activity.
	IT network administrator	No activity.
	Field operator	No activity.

General description: which actor does what	The sensor is mounted in a machine. The sensor includes the correct parameter(s). The sensor and the machine work adequately. The attacker has physical access to the sensor (push-buttons), which is mounted in a machine. The sensor is not protected against re-configuration of the parameters. The attacker is able to modify the sensor with improper value(s) of the parameter(s) by using the push-buttons. The unauthorized re-configuration of the parameters could be undetected over a long time, depending on the application. The unauthorized re-configuration of the sensor will be found out, when a critical condition in the process is achieved, e.g. maximum level in a tank is reached and the sensor generates no detection signal.	
Detail description: trigger, steps relating to how actors are working together, etc.	Attacker	The attacker has access to the manual of instructions, e.g. manufacturer homepage (optional). The attacker gains access to the sensor, mounted in a machine. The attacker activates the programming mode (knowingly or by trial-and-error method). The attacker manipulates the parameter(s). The attacker enables the parameter(s) or the sensor automatically enables the parameter(s). The attacker departs from the machine undetected.
Countermeasures	Manufacturer	There are no suitable countermeasures. Duty to supply information: the manufacturer shall state in the product documentation (e.g. manual of instructions): – that no security countermeasures are integrated in the sensor; – suitable integration method such as with an additional accessory for limiting the access to the push-button of the machine.
	Integrator/User	The integrator and the operator are obliged to take appropriate security countermeasures according to the operator's specifications and legal requirements.

B.8 Use case 7 – HMI: human machine interface – Protection against unauthorized access to a complex sensor (mounted in a machine) – improper parametrization

Name of use case	HMI: human machine interface – Protection against unauthorized access to a complex sensor mounted in a machine – improper parametrization.	
Lifecycle	Operation with a minimum level exposure E2 (CF1, C2) according to Table 2.	
Phase	Active phase of machinery.	
Objective and benefit for whom	To ensure the continuity and validity of information/data and function. Benefit for operator company, operator and manufacturer of the sensor: reliable function of the machine, no customer complaints. The use case describes a complex sensor equipped with push-buttons and a display and accessible via a data interface for programming the parameters and locking the push-buttons.	
Actors	Attacker/ Aggressor	Attacker who tries to modify the specified and configured sensor parameter(s) for this application.
	Manufacturing automation manager	No activity.
	Service operator	No activity.
	IT network administrator	No activity.
	Field operator	No activity.

General description: which actor does what	The sensor is mounted in a machine. The sensor includes the correct parameter(s). The sensor and the machine work adequately. The attacker has physical access to the sensor. The sensor is not protected against re-programming. The attacker is able to modify the sensor with faked parameter(s). The unauthorized re-programming could be undetected over a long time, dependent on the application. The unauthorized re-programming of the sensor will be found when a critical condition in the process is achieved, e.g. maximum level in a tank is reached and the sensor generates no output signal.	
Detail description: trigger, steps relating to how actors are working together, etc.	Attacker/ Aggressor	The attacker has access to the manual of instructions, e.g. manufacturer homepage (optional). The attacker gains access to the sensor by corrupting the infrastructural safety measures. The attacker gains knowledge of the access options of the sensor. The attacker logs into the programming interface with a default or disclosed password and an ID. The attacker activates the parameter setting mode. The attacker manipulates the parameters. The attacker enabled the parameter(s) or the sensor automatically enabled the parameter(s).
Countermeasures	Manufacturer	Install user access control measure, for example user name(s) and password(s). Examples of access control implementation: – delay in case of wrong password input; – delay in case of restart; – encrypt remote access; – deactivate local sensor push-buttons; – logging x unsuccessful login attempts; – prevent access after logging x unsuccessful login attempts; – user account management (rights/roles); – make the password changeable; – minimum password complexity; – make it mandatory to change initial passwords; – no function without prior password change; – input validation; – use of connection-oriented protocols; – predetermined states of the outputs; – implement basic security feature based on this document.
	Integrator/ User	The integrator/user should create and document an authorization concept. The integrator/user should implement the aspects indicated above to the best of his knowledge according to the authorization concept. The integrator and the user are obliged to take appropriate security countermeasures according to the operator's specifications and legal requirements.

B.9 Use case 8 – Protection against unauthorized access to a sensor (e.g. proximity switch), mounted in a machine, connected by wireless communication interface (WCI)

Name of use case	Protection against unauthorized access to a sensor (e.g. proximity switch), mounted in a machine, connected by wireless communication interface.	
Lifecycle	Operation, maintenance with a minimum level exposure E3 (CF1, C3) according to Table 2.	
Phase	Active phase of machinery.	
Objective and benefit for whom	To ensure the continuity and validity of information/data and function. Benefit for operator company, operator and manufacturer of the sensor: reliable function of the machine, no customer complaints. This use case is also valid within a smart manufacturing system.	
Actors	Hacker	The hacker tries to get access to the transferred data/information of the sensor via WCI (reading and modification of the data/information)
	Manufacturing automation manager	No activity.
	Service operator	No activity.
	IT network administrator	He is responsible to ensure that only authorized devices have access to the WCI.
	Field operator	No activity.
General description: which actor does what	The hacker has the required technical equipment. He has the required know-how. He is within network range. He gains access to the wireless network: a) he reads data/information; b) he changes data/information and transmits it to the recipient; c) the sensor is influenced so that it fails (causes a complaint with the sensor manufacturer).	
Detail description: trigger, steps relating to how actors are working together, etc.	Hacker	He overcomes existing authentications. The implementation on the radio chip has a security flaw, the wireless protocol allows for intrusions. Or he gains access to the password. a) He reads data/information. This is not detected; b) He changes data/information and transmits it to the recipient. This is not detected; c) The sensor is influenced so that it fails. He superimposes the communication channel with a sensor featuring a higher performance. This is detected and causes a complaint with the manufacturer.